Correlation of conflicts in distributed special-purpose management systems

Serhii Stefantsev [*A]

[*]**Corresponding author:** Senior Lecturer, e-mail: stefancevss@kneu.edu.ua, ORCID: 0000-0002-7629-7563
[A] Kyiv National Economics University named after Vadym Hetman, 54/1, Peremogy Ave., Kyiv, 03057, Ukraine

Received: December 03, 2020 | Revised: December 15, 2020 | Accepted: December 31, 2020

DOI: 10.5281/zenodo.4399916

Abstract

One of the mandatory conditions for the successful implementation of any innovative project is to reliably ensure its information security. The specifics of innovation and venture activities, as a rule, involve the widespread use of modern information technologies for managing organizational production and technological processes, which (if the information security system is imperfect) may be associated with certain risks. This makes it relevant to introduce a methodological apparatus for correlating threats and supporting management decision-making to ensure the availability, confidentiality, and reliability of the information. When managing processes in the information sphere, quite often there is a need to decide in weakly structured situations, when the parameters, laws, and regularities of the development of the situation are described not quantitatively, but qualitatively. At the same time, a unique situation arises when changes in its structure are very difficult to predict. Therefore, the article deals with the issue of cognitive analysis of conflicts in distributed special-purpose management systems, considers concepts that affect the security of software, builds a fuzzy cognitive map of the model of information security risk formation, quantifies the impact of cognitive modeling conflicts in distributed special-purpose management systems, and analyzes the results of calculations and justifies the results.

Key words: information security, information security risk formation model, fuzzy cognitive map, software, distributed special-purpose management systems, information security systems.

Introduction

Today, the most popular information security systems are those that allow you to increase the degree of intelligence of existing security mechanisms: firewalls, security scanners, and intrusion detection systems, access control tools for operating systems and application programs. In the field of Information Security Event Management, a new category of security systems has been developed that implements the concept of Security Event Management (Garusi, M., 2003; Fedorchenko, A. V., 2020). These systems automatically combine and coordinate corporate security registration data obtained from various security devices, evaluate their correlation, allowing information security analysts to focus on non-trivial critical tasks. Concerning information protection, we can say that correlation is the process of interpreting, combining, comparing, and analyzing data coming from various information security mechanisms, which is carried out to determine attempts of unauthorized access to protected information resources or attacks on them. At its core, event correlation is based on the following theoretical premise: one event that occurs over a certain period is the cause of another event. In the technological process of correlation of security events, the following tasks are distinguished: data Transportation; data normalization; compression (reduction) of data; building a chain of events; identifying patterns in events; establishing the relationship between information security events. In general, all event

correlation systems transform the flow of information security events into useful information containing data on the state of the information infrastructure and vulnerabilities identified in its environment. This information is presented to the security administrator for decision-making.

In distributed special-purpose control systems, digital systems for monitoring and/or managing real objects of various nature and purpose are considered (Liashenko, I. O., 2013).

The main features of distributed special-purpose control systems include:

- real-time operation;
- special requirements for reliability and safety of operation;
- continuous operation mode;
- almost constant absence of the operator and the need to solve emergencies by the distributed special-purpose control system itself.

Accordingly, a distributed special-purpose management system is understood as digital self-purpose management systems for solving problems in a particular subject or departmental Area (Stepanova, A. S., Muromtsev, D. Yu., 2009).

Summarizing the above, we formulate the definition: a distributed control system for special purposes is a multi-level hierarchical computing system that is designed to automate the control and management in a complex technical system of some real object in a certain subject or departmental area in real-time operation conditions, in the presence of high requirements for reliability and safety of operation during continuous operation and the possibility of temporary absence of the operator. It is quite obvious that it is in distributed special-purpose management systems that weakly structured unique situations typical of monitoring and management tasks in the administrative and socio-political spheres are the most difficult to analyze and support decision-making.

Analysis of recent research and publications. In the existing mechanisms of correlation of security events, the approaches of Mukhin V. E. and Volokit A. N. (2009), Kozlova E. A. (2013), Fedorchenko A.V. (2016) are used: correlation based on rules, correlation-based on modeling, correlation based on the codebook method, correlation using intelligent methods (Fedorchenko, A. V., 2020; Kozlova, E. A., 2013; Mukhin, V. E., Volokita, A. N., 2009). Each of these methods has several disadvantages that limit its use in real or routine time. According to information security experts, today the correlation stage is a critical part of the complex threat analysis process (Garusi, M., 2003). This is because within the framework of the classical approach, which is based on the installation of a large number of unrelated security tools, it is impossible to provide analysts of the information security service with complete information about the attack, which they must study and rank according to the degree of importance. At the same time, correlation technology is the development of a holistic approach to Threat Management in a heterogeneous environment and requires significant resources of a distributed special-purpose management system.

Problem statement. The purpose of the article is to conduct a cognitive analysis of conflicts in distributed special-purpose control systems. To perform the analysis, it is necessary to build a fuzzy cognitive map of the information security risk formation model in the form of an oriented graph that formally reflects cause-and-effect relationships without taking into account the intensity of mutual influence of concepts. Based on the results of quantitative assessment of the strength of the influence of concepts on each other, it is necessary to construct a matrix of mutual influences of concepts of a fuzzy cognitive map of the subject area and analyze the results obtained.

Material and methods

The basis for setting and solving problems of determining the correlation of information security events is the theory and methods of modeling, mathematical statistics, and expert assessments (Fedorchenko, A. V., 2020; Avetisyan, A. I., 2014; Nadezhdin, E. N., 2017). Software vulnerabilities will be understood as critical errors that were not detected during

testing and are not declared by the developer's specification, or are intentionally embedded, providing attackers with exceptional opportunities to disclose information, modify it, block it, use it, and finally destroy it without the possibility of recovery (Avetisyan, A. I., 2014).

Analysis of modern methods (Taze, A., 1990; Bidoit, N., Hull, R., 1989) suggests that the most convenient mathematical apparatus for describing and studying distributed control systems for special purposes is fuzzy cognitive modeling. The indisputable advantages of fuzzy cognitive modeling in comparison with other methods are the ability to formalize numerically non-comparative factors, the use of incomplete, fuzzy and even contradictory information. The fuzzy cognitive model is based on the formalization of causal relationships between factors (variables, parameters) that characterize the system under study. The result of formalization is a mapping of the system in the form of causal relationships, which is called a fuzzy cognitive map. Building a fuzzy cognitive map of a managed system actually means removing uncertainty from its structure by forming a knowledge model of the person making decisions about that system. Analytical processing methods are applied to the constructed map, focused on studying the structure of the system and obtaining a forecast of its behavior under various control influences in order to find optimal control strategies (Liashenko, I. O., 2020).

Results and discussion

Cognitive analysis of conflicts in distributed special-purpose management systems

Fuzzy cognitive maps provide a correct formal display of a weakly structured subject area and acceptable accuracy of Process Modeling in comparison with classical cognitive maps. The concept of a fuzzy cognitive map by V. B. Silov is an extension of the classical concept of a cognitive map, based on the assumption that mutual influences between concepts can differ in intensity, their intensity can change over time (Silov, V. B., 1995). To do this an indicator of the intensity of exposure is entered in fuzzy cognitive maps and the classical ratio is switched to a fuzzy *W* ratio, elements w_{ij} which are characterized by the direction and degree of intensity (weight) of influence between concepts e_i i e_j:

$$w_{ij} = w(e_i, e_j), \quad (1)$$

where *w* is the normalized indicator of the intensity of exposure (a characteristic function of the ratio *W*), which has a number of special properties.

A fuzzy cognitive map displays the object under study as a weighted oriented graph, the vertices of which correspond to the elements of the set *E* (concepts), and arcs – nonzero elements of the relationship *W*, that is, causal relationships. Each arc has a weight specified by the corresponding value w_{ij} The ratio *W* is represented as a cognitive Matrix $W = \{w_{ij}, i, j = \overline{1,n}\}$ dimensions ($n \cdot n$) (n – number of concepts in the system), which will be interpreted as the adjacency matrix of this graph. The state of the system at the current time is determined by a set of values for all concepts of the fuzzy cognitive map. The target state of the system is defined by the value vector of a set of target concepts.

1. Concepts that affect software security. With an integrated approach to building a model of information security risk formation for a distributed special-purpose management system based on a cognitive model, first of all, it is necessary to form a set of concepts-the most significant factors from the point of view of studying this problem. Analyzing the data obtained as a result of an expert survey, to build a fuzzy cognitive map of the information security risk formation model, we will use the list of the most common software defects (vulnerabilities and inaccuracies) (Avetisyan, A. I., 2014) and identify concepts that affect the security of software:

- e_1 – External attacks.
- e_2 – Internal attacks.
- e_3 – Buffer overflow.

• e_4 – Errors when working with dynamic memory.

• e_5 – Software bookmarks.

• e_6 – Data leaks; violation of the integrity of information resources.

• e_7 – Compiler-level protection.

• e_8 – Compiler-level protection. Special tools for protecting system and application resources.

• e_9 – Obfuscation (entanglement) system.

• e_{10} – Monitoring the integrity of executable programs based on analyzing their activity and updating them.

• e_{11} – Quality of software functioning.

• e_{12} – Information security risks caused by software health problems.

The next step is to determine the strength of the connection that determines the influence of one concept on another and is determined by linguistic terms. The relationships between concepts in a fuzzy cognitive map can be as positive as possible — enhancing the impact of the concept e_i on the concept e_j ($w_{ij} \succ 0$), yes and negative — those that weaken the influence of the concept e_i on the concept e_j ($w_{ij} \prec 0$),that is $w_{ij} \in [-1;1]$.

To solve this problem, we will set a fuzzy linguistic scale: communication strength = {does not affect; very weak; weak; medium; strong; very strong}. Each of these terms corresponds to a numerical range belonging to the segment [0, 1] for positive relations:

$$w_{ij} = \begin{Bmatrix} 0, \text{ does not affect;} \\ (0; 0{,}15], \text{ very weak;} \\ (0{,}15; 0{,}35], \text{ weak;} \\ (0{,}35; 0{,}6], \text{ medium;} \\ (0{,}6; 0{,}85], \text{ strong;} \\ (0{,}85; 1], \text{ very strong.} \end{Bmatrix},$$

and a similar numeric range is taken with opposite signs, which belongs to the segment [-1, 0].

Based on the processing of data obtained as a result of an expert survey, we will determine the strength of the relationship between each pair of concepts, which corresponds to a numerical estimate.

The development by experts in the field of Information Technology of a knowledge structure about the information security system, a list of concepts of influence on software security, and the strength of communication between these concepts allows us to build a fuzzy cognitive map of the information security risk formation model (fig. 1).

2. Building a fuzzy cognitive map of the information security risk formation model. Modeling was performed using Mental Modeler software tools (Gray, S. A., 2020).

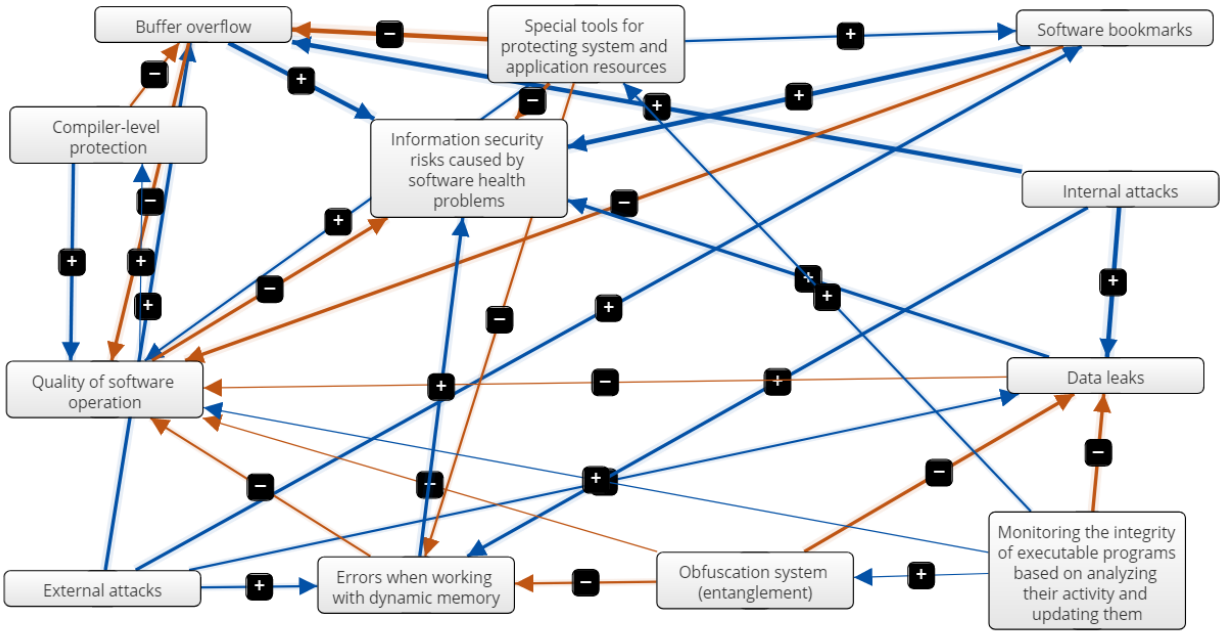

Fig. 1. Fuzzy cognitive map of the information security risk formation model

3. Quantification of the impact of cognitive modeling conflicts in distributed special-purpose control systems. After analyzing the causal relationships between the concepts, we note that the developed fuzzy cognitive map contains:

- three "Driver" concepts – affect other concepts, but they are not affected by any of the system concepts;

- one "Receiver" concept – it is influenced by system concepts, but it does not affect any of them;

- eight concepts of the "Ordinary" type – ordinary, intermediate concepts that are influenced and influenced by certain concepts of the system.

Matrix $W = \{w_{ij}, i, j = \overline{1,12}\}$ the mutual influence of the concepts of this fuzzy cognitive map will have the following form (table. 1).

Table 1 – Matrix of mutual influences of concepts of a fuzzy cognitive map of the subject area

	External attacks	Internal attacks	Buffer overflow	Software bookmarks	Data leaks	Compiler-level protection	Special tools for protecting system and application resources	Obfuscation system (entanglement)	Monitoring the integrity of executable programs based on analyzing their activity and updating them	Quality of software operation	Information security risks caused by software health problems	Errors when working with dynamic memory
External attacks			0.71	0.7	0.25							0.2
Internal attacks			0.88		0.85							0.75
Buffer overflow										-0.77	0.86	
Software bookmarks										-0.54	0.87	
Data leaks										-0.08	0.73	
Compiler-level protection			-0.34							0.55		
Special tools for protecting system and application resources			-0.89	0.29						0.34	-0.82	-0.37
Obfuscation system (entanglement)					-0.57					-0.03		-0.37
Monitoring the integrity of executable programs based on analyzing their activity and updating them					-0.54		0.22	0.09		0.11		
Quality of software operation						0.08					-0.68	
Information security risks caused by software health problems												
Errors when working with dynamic memory										-0.43	0.7	

To determine the structural and topological properties of the resulting fuzzy cognitive map, we use the following indicators of the structural complexity of the fuzzy cognitive map:

• fuzzy cognitive map density – shows the degree of connectivity of the graph that displays this fuzzy cognitive map:

$$d = \frac{m}{n(n-1)}, \quad (2)$$

where *m* is the total number of connections of the fuzzy cognitive map, and *n* is the total number of concepts of the fuzzy cognitive map.

In our case, *n* = 12, *m* = 31, substituting the corresponding values in Formula (2), we get that *d* = 0,235. this value indicates a fairly large number of connections between concepts, that is, a high density of the developed fuzzy cognitive map.

• centrality of the concept – characterizes the degree of interaction of the *i*-th concept of a fuzzy cognitive map with its neighbors:

- initial centrality – shows the total strength of connections (w_{ij}), based on the concept under consideration e_i:

$$od_i = \sum_{j=1}^{n} w_{ij}, \quad (3)$$

- input centrality – shows the total strength of connections (w_{ij}), what are included in the analyzed concept e_i:

$$id_i = \sum_{j=1}^{n} w_{ij}, \quad (4)$$

- general centrality of the concept:

$$td_i = od_i + id_i. \quad (5)$$

Calculation of centrality indicators has shown that the concept of e_{12} has the highest structural significance ($td_6 = 4{,}66$),as well as concepts e_3, e_6, e_{11} (indicators td_3, td_6, td_{11} equal respectively 4.45; 3.02; 3.61). These concepts accumulate the greatest number of connections from other concepts, that is, they play the role of peculiar centers of influence in a fuzzy cognitive map in the model of information security risk formation.

• complexity – represents the ratio of the number of concepts of the "Receiver" type to concepts of the "Driver" type. The higher the value of this coefficient, the more complex the maps are since it is assumed that they contain more useful results and fewer controlled impacts on the external environment.

For the developed fuzzy cognitive map of the subject area we, obtain the relation: $\frac{1}{3} \approx 0{,}33$, which indicates insufficiently complex thinking systems.

• hierarchy index (*h*):

$$h = \frac{12 \cdot \sigma_{od}^2}{n^2 - 1}, \quad (6)$$

де $\sigma_{od}^2 = \frac{\sum_{i=n}^{n} (od_i - \mu_{od})^2}{n}$, $\mu_{od} = \frac{\sum_{i=n}^{n} od_i}{n}$.

For *h* = 1, the system is completely hierarchical, and for *h* = 0, it is completely democratic. Democratic systems are more adaptive to changes in the external environment due to their high level of integration and connectivity. In our case, *h* = 0.2, which indicates a high democratic nature of the system under study.

In Table. 2 shows the quantitative value of the main system indicators of the developed fuzzy cognitive map of the subject area: consonance, dissonance and the influence of concepts on the system.

Table 2 – Main indicators of a fuzzy cognitive map of the subject area

Component	Indegree	Outdegree	Centrality
External attacks	0	1.8599999999999999	1.8599999999999999
Internal attacks	0	2.48	2.48
Buffer overflow	2.82	1.63	4.449999999999999
Software bookmarks	0.99	1.4100000000000001	2.4000000000000004
Data leaks	2.21	0.8099999999999999	3.02
Compiler-level protection	0.08	0.8900000000000001	0.9700000000000001
Special tools for protecting system and application resources	0.22	2.71	2.93
Obfuscation system (entanglement)	0.09	0.97	1.06
Monitoring the integrity of executable programs based on analyzing their activity and updating them	0	0.96	0.96
Quality of software operation	2.85	0.76	3.6100000000000003
Information security risks caused by software health problems	4.66	0	4.66
Errors when working with dynamic memory	1.69	1.13	2.82

After analyzing the above indicators, we will determine the most influential concepts of the system under study (those concepts that have the greatest value of consonance (outdegree) and influence on the system): e_2 – Internal attacks; e_8 – Special tools for protecting system and application resources; e_1– External attacks; e_3 – Buffer overflow.

Analysis of calculation results and justification of results. At this stage, we will

conduct scenario modeling to determine the relative change in the level of security of the system with the maximum value of the impact of the most significant concepts on it.

Scenario 1. State of the concept e_2 – Internal attacks are activated by taking the maximum possible negative value.

Note that the organizational component of "Internal attacks" plays a significant role in creating a reliable integrated security mechanism. After all, most threats are caused not by technical aspects, but by the actions of intruders, carelessness, or mistakes of personnel. Therefore, it is important to get a forecast for the development of this situation.

The concept $e_2$in the developed fuzzy cognitive map, it has a direct impact on the components: e_3 – Buffer overflow; e_4 – Errors when working with dynamic memory; e_6 – Data leaks; violation of the integrity of information resources. Therefore, when changing the value e_2 such a reaction of the system under study will be observed (fig. 2).

The resulting bar chart shows that internal attacks will increase the value of concept e_{11} – the quality of software functioning, which in turn will lead to a decrease in buffer overflow by 0.3; data leaks; violation of the integrity of information resources by 0.28; information security risks caused by software health failure by 0.16; errors when working with dynamic memory by 0.26.

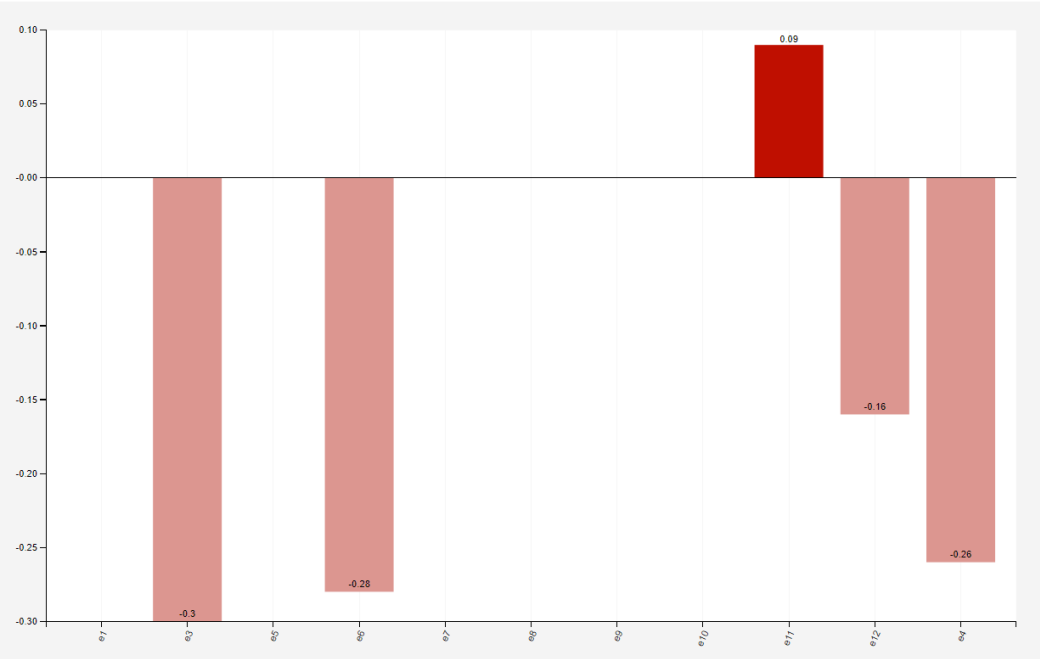

Fig. 2. A scenario that reflects the system's response

Scenario 2. Maximum reduction of the concept value e_8 – Special tools for protecting system and application resources.

In the model under study, the concept e_8 – Special tools for protecting system and application resources have a direct impact on concepts e_3 – Buffer overflow; e_4 – Errors when working with dynamic memory; e_5 – Software bookmarks; e_{11} – Quality of software functioning and e_{12} – Information security risks caused by software health problems. The most negative change in the value will lead to this situation (fig. 3).

After analyzing the resulting histogram, we can draw conclusions about the relative change in the concepts of the developed fuzzy cognitive map, which are affected by e_8. In particular, there is a decrease in Bookmark programs by 0.11; the quality of software functioning – by 0.15.

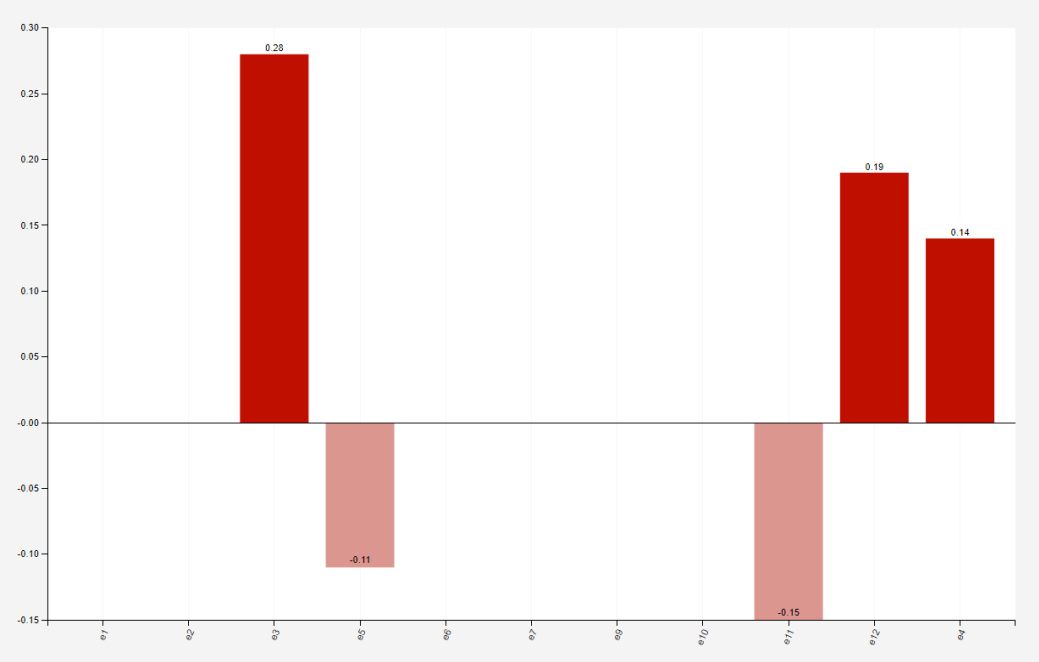

Fig. 3. A scenario that reflects the system's response to maximum negative changes in the concept e_8

Scenario 3. Maximum reduction of the value of the concept e_1– External attacks.

In the constructed fuzzy cognitive map the concept of e_1 – External attacks directly affect such concepts: e_3 – Buffer overflow; e_4 – Errors when working with dynamic memory; e_5 – Software bookmarks; e_6 – Data leaks; violation of the integrity of information resources. The system's response to a negative increase in the value of this concept is shown in Fig. 4.

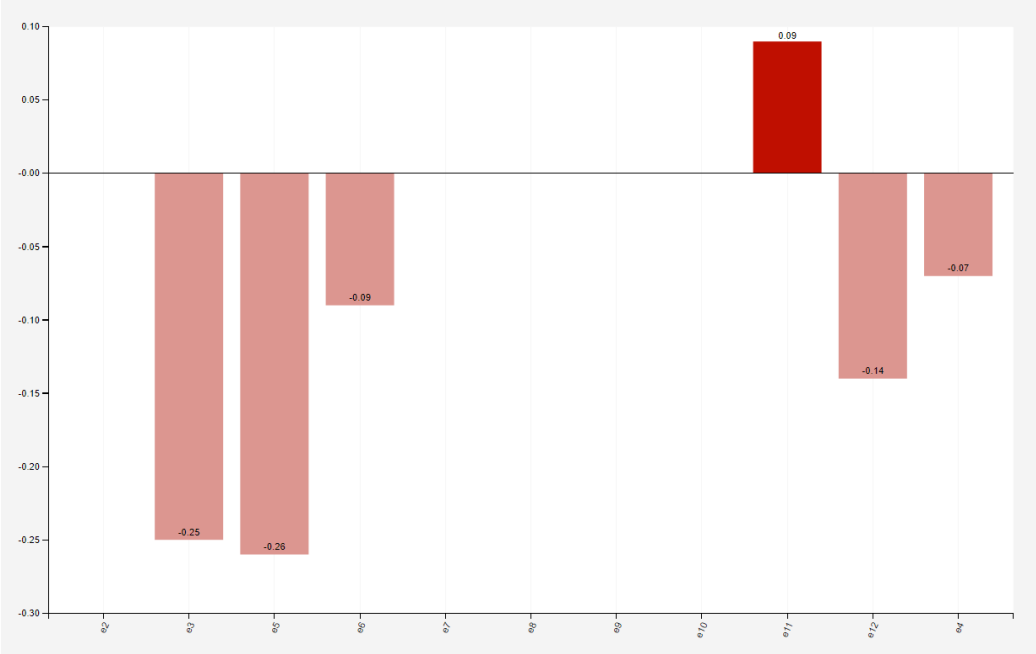

Fig. 4. A scenario that reflects the system's response to maximum negative changes in concept e_1

As a result of modeling this scenario, we see that buffer overflows will weaken by 0.25; errors when working with dynamic memory – by 0.07; software bookmarks by 0.26; data leaks; violation of the integrity of information resources by 0.09; information security risks caused by software health failure by 0.14.

Analysis of the results of cognitive analysis allows us to identify concepts that positively and negatively affect the component of information security risk caused by the vulnerability of software and, in part, information support of a distributed special-purpose management system. Concepts e_1 and e_2, describing external and internal sources of information attacks, within the framework of the proposed model, they do not experience targeted influence from the information security system. Similarly, you can point to the concept of e_{10}, which in our case is an autonomous tool for monitoring and controlling the quality of software functioning. It should also be noted that violations of the integrity of information resources can be the result of well-prepared external and internal attacks carried out by agreement or independently.

Conclusions

Based on the results of the conducted cognitive analysis, it can be assumed that the biggest positive effect should be expected from a coordinated change in the group of controlled concepts of the fuzzy cognitive map, which are in the chain of causal relationships and together provide a stable impact on the system – model of information security risk formation.

The model of information security risk formation caused by the implementation of information attacks through characteristic vulnerabilities in the software of a distributed special-purpose management system allows us to solve some Applied Problems that are characteristic of the correlation of information security events. Despite the enlarged nature of the model and the simplified cognitive display of relationships between concepts, the proposed approach can identify significant relationships between vulnerable and specific software protection mechanisms.

The formal presentation of the information security risk formation model in the form of a fuzzy cognitive map allowed us to systematize knowledge of the subject area, statistical data on information security incidents and expert experience in the interests of identifying patterns and quantifying the degree of correlation of heterogeneous vulnerabilities and protection measures to information security risks.

The results of the study can become a methodological basis for choosing the direction of modernization of the existing security event management system to fully meet the requirements of corporate security policy in conditions that change the characteristics of external and internal threats.

Prospects for further research. A perspective way of further research is the development of a new information technology to ensure the necessary level of efficiency in the functioning of the decision support system in distributed special-purpose management systems at the stages of their creation and operation.

References

Avetisyan, A. I., Belevantsev, A. A., Chuklyaev I. I. (2014). The technologies of static and dynamic analyses detecting vulnerabilities of software. *Cybersecurity*. issues, 3(4), 20-28. Retrieved November 08, 2020 Available from: https://cyberleninka.ru/article/n/tehnologii-staticheskogo-i-dinamicheskogo-analiza-uyazvimostey-programmnogo-obespecheniya.

Bidoit, N., Hull, R. (1989). Minimalism, justification and non-monotony in deductive databases. Journal of Computer and System Sciences, 38, 290-325. Retrieved November 08, 2020. DOI: 10.1016/0022-0000(89)90004-4.

Brewka, G. (1991). Nonmonotonic Reasoning: Logical Foundations of Commonsense. Cambridge University Press. Retrieved November 08, 2020. DOI: 10.1017/S026988890000014X.

Brewka, G., Dix, J., Konolige, K. (1997). Nonmonotonic Reasoning – An Overview. Stanford: CSLI publications.

Cadoli, M., Schaerf, M. (1993). A survey of complexity results for non-monotonic logics. The Journal of Logic Programming, 17, 127-60. Retrieved November 08, 2020. DOI: 10.1016/0743-1066(93)90029-G.

Donini, F.M., Lenzerini, M., Nardi, D. et al. (1990). Nonmonotonic reasoning. Artif Intell Rev 4, 163-210. Retrieved November 08, 2020 DOI: 10.1007/BF00140676.

Fedorchenko, A. V., Levshun, D. S., Chechulin, A. A., & Kotenko, I. V. (2016). An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. SPIIRAS Proceedings, 6(49), 208-225. Retrieved November 08, 2020. Available from: DOI: 10.15622/sp.49.11.

Garusi, M. (2003) Event correlation systems: revolution or evolution? *Network online*, #7, 7-11.

Ginsberg, M. L., ed. (1987). Readings in Nonmonotonic Reasoning. Los Altos CA: Morgan Kaufmann.

Gray, S. A., S. Gray, J. L. De Kok, A. E. R. Helfgott, B. O'Dwyer, R. Jordan, and A. Nyaki. (2015). Using fuzzy cognitive mapping as a participatory approach to analyze change, preferred states, and perceived resilience of social-ecological systems. Ecology and Society 20(2): 11. Retrieved November 08, 2020. http://dx.doi.org/10.5751/ES-07396-200211.

Horty, J. F. (2001). "Nonmonotonic Logic," in Goble, Lou, ed., The Blackwell Guide to Philosophical Logic. Blackwell.

Kozlova, E. A. (2013). Information security risk assessment using the method of fuzzy clustering and mutual information calculation. *Young scientist*, 5 (52), 154-161. Retrieved November 08, 2020. Available from: https://moluch.ru/ archive/52/6967/.

Liashenko, I. O., Stefantsev, S. S., Polumiienko, S. K. (2020). Fuzzy cognitive models in decision support tasks of distributed special purpose control systems. InterConf, (9). Retrieved November 08, 2020 Available from: https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/1214.

Liashenko, I. O., Voitko, O. V., Chernega, V. M., Rakhimov, V. V. (2019). Formal model of Decision Support in poorly structured situations of a distributed management system. Proceedings of the XV International Scientific and Practical Conference International Trends in Science and Technology. Publisher – RS Global Sp. z O.O., Warsaw, Poland. Vol. 1, July 31, 2019, P. 36-40. ISBN 978-83-954081-6-8. Available from: http://ws-conference.com/.

Liashenko, I. O. (2013). Selection of survivability indicators for special-purpose information and control systems. Information processing systems, 2, 64-66. Retrieved November 08, 2020 Available from: http://nbuv.gov.ua/UJRN/ soi_2013_2_16.

Mukhin, V. E., Volokita, A. N. (2009). Analysis of information security events to perform corrective actions for security management. *Computer science, management and engineering*, 50, 1–7. Retrieved November 08, 2020. Available from: https://ela.kpi.ua/handle/123456789/8116.

Nadezhdin, E. N., Novikova, T. L. (2017). Optimization of vulnerability search in the system of protection of University information and computer network resources. *Modern high-tech technologies*, 4, 38-43. Retrieved November 08, 2020. Available from: http://www.top-technologies.ru/ru/article/view?id=36636.

Silov, V. B. (1995). Making strategic decisions in a fuzzy environment. Moscow: INPRO-RES. Retrieved November 08, 2020. Available from: http://www.padaread.com/?book=30006&pg=1.

Stepanova, A. S., Muromtsev, D. Yu. (2009). The analysis of information-operating systems evolution with the use of scientifically-technological foresight. Samara: proceedings of the Samara scientific center of the Russian Academy of Sciences, 354-357. Retrieved November 08, 2020. Available from: https://cyberleninka.ru/article/n/analiz-razvitiya-informatsionno-upravlyayuschih-sistem-s-ispolzovaniem-nauchno-tehnologicheskogo-forsayta/viewer.

Taze, A., Gribaumont, P., Louis J. (1990). Logical approach to artificial intelligence: From classical logic to logical programming. Moscow: World. Retrieved November 08, 2020. Available from: http://www.aiportal.ru/downloads/books/logical-approach-to-ai-by-tei-gribomon-and-other.html.